JAK OVLÁDNOUT IEC 62443

Pokročilé metody kybernetické bezpečnosti pro průmysl a kritickou infrastrukturu

Helena Hrašková & Ilja David ☆ SCADA Security konference ☆ České Budějovice ☆ 2024

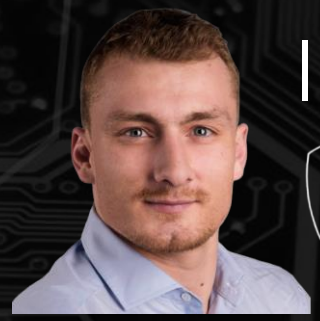
KDO JSME

Helena Hrašková

COMGUARD

cyber security masters

Helena působí v roli obchodní konzultantky a produktové manažerky u distributora COMGUARD a.s, který působí jako Value Added Distributor v oblasti kybernetické bezpečnosti. Úzce spolupracuje s výrobci a obchodními partnery a ve své obchodní profesi se zaměřuje výhradně na kybernetickou bezpečnost.
V Comguardu je zodpovědná za oblast kybernetické bezpečnosti v průmyslovém prostředí.



Ilja David

IRON OT

Secure The Industry Future

Více než 10 let zkušeností s průmyslovou kybernetickou bezpečností obsahuje praktické projekty v klíčových průmyslových odvětvích, jako je letecký, námořní, potravinářský, energetický, ropný a plynárenský, farmaceutický, chemický a to ve společnostech Airbus Defence and Space, DNV a Nestlé, kde byl mmj. regionální manažer IT bezpečnosti pro 130 továren v 62 zemích.

Obsah

1# OT Cyber Incident

2# Operational Technologies

3# Standardy IEC 62443

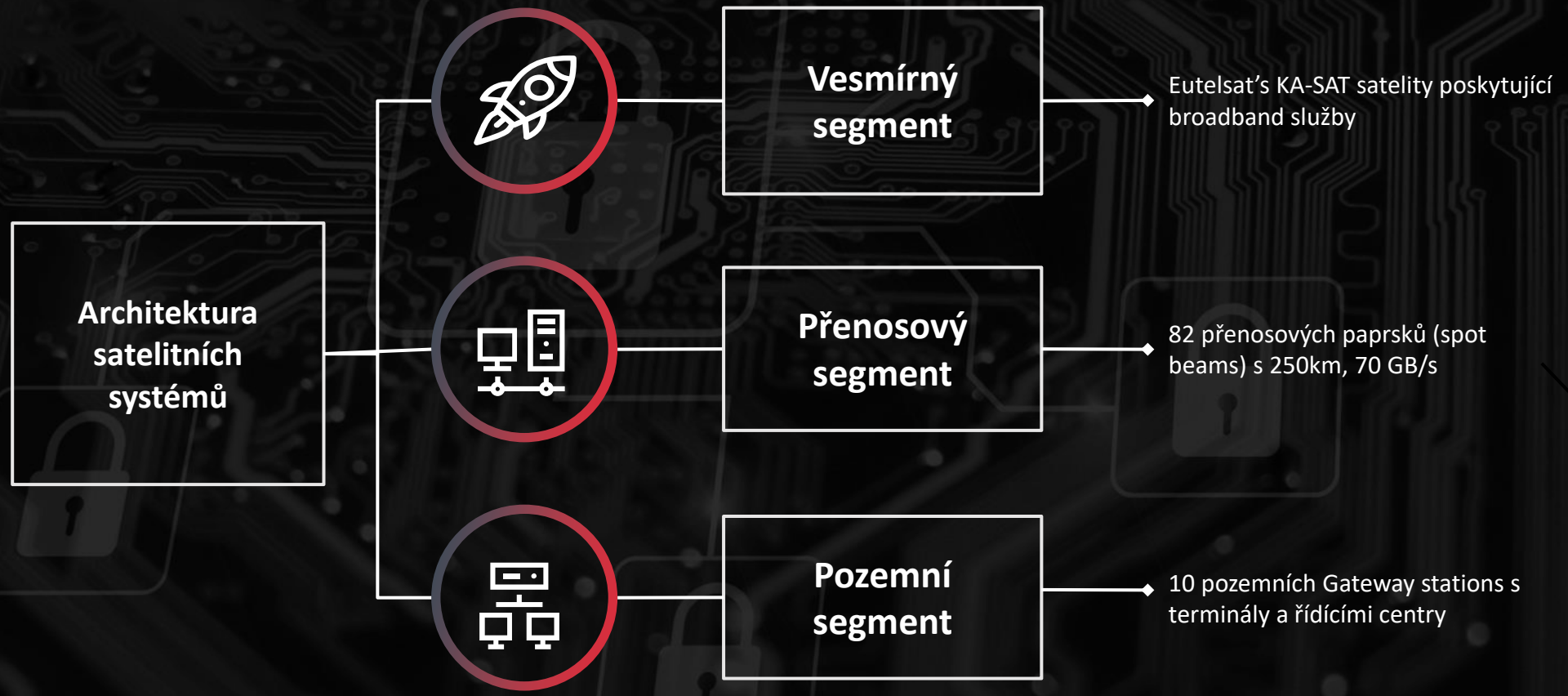
4# Bezpečná architektura

5# Shrnutí

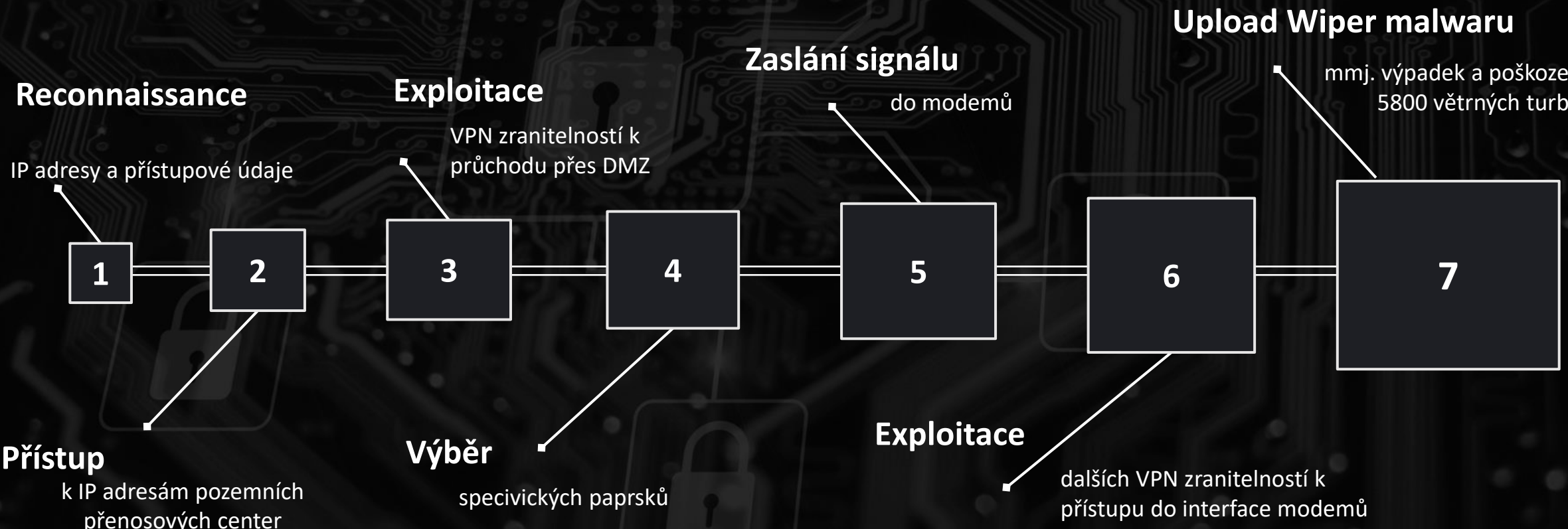
1# Cyber Incident

Ponaučení z kybernetického incidentu na spol. Viasat

Viasat Cyber-Attack Complexity



Viasat Cyber-Attack Chain



~5800

nefunkčních větrných turbín

Viasat Cyber-Attack Lessons Learned

Supply Chain Management

Absence znalosti zapojení třetích stran

Absence řízení rizik „dual-use“ tech.

Žádné audity třetích stran

Proaktivní monitoring

Zranitelná zařízení nebyla monitorována

Předchozí úniky dat nebyly zjištěny

Nedefinovány kritické komponenty

Patch management

Nepatchovaná zařízení

Software i firmware

Nekonzistence patch procesu

Incident response

Absence redundance

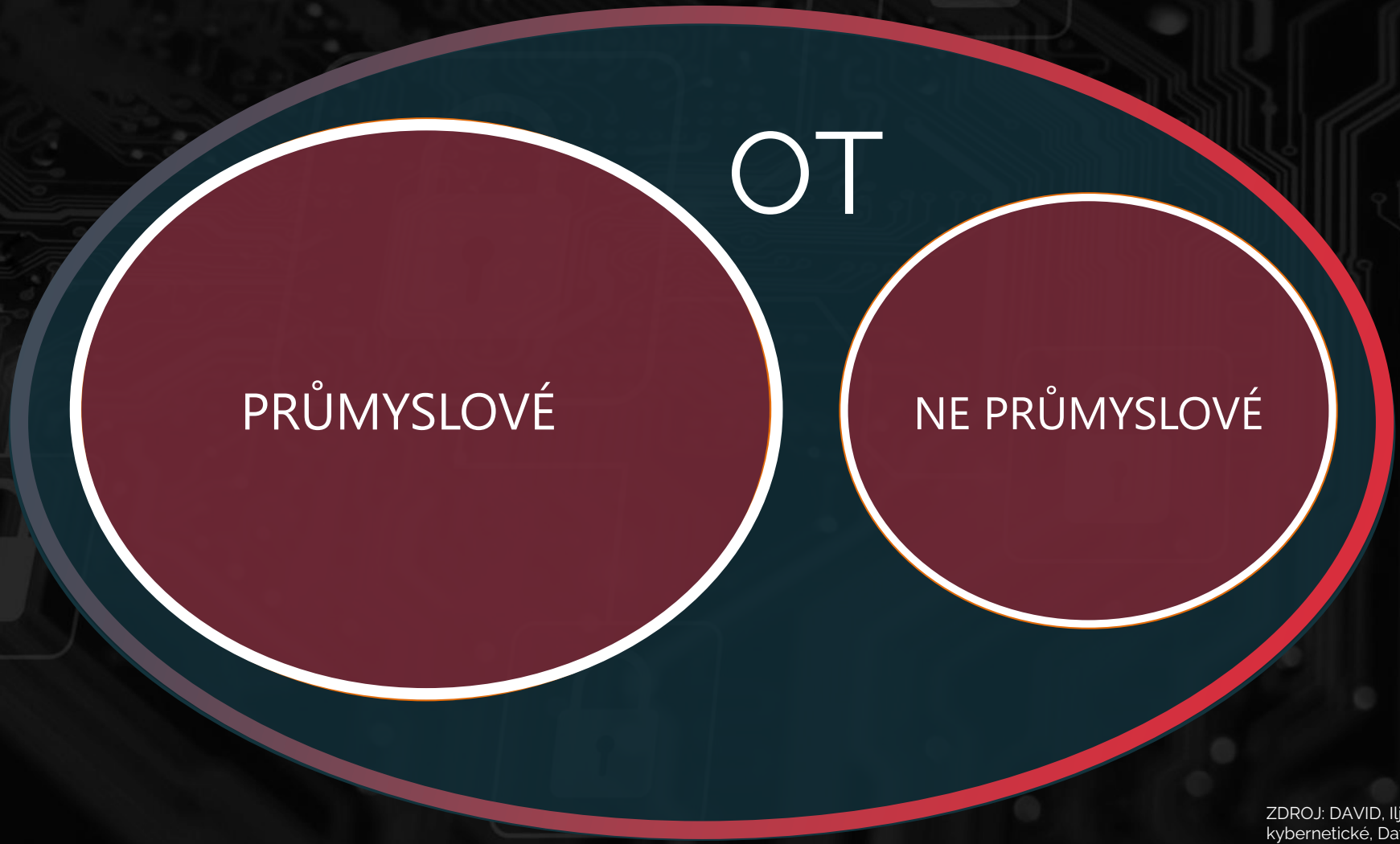
Žádný incident response proces

Absence BCP

2# Operational Technologies

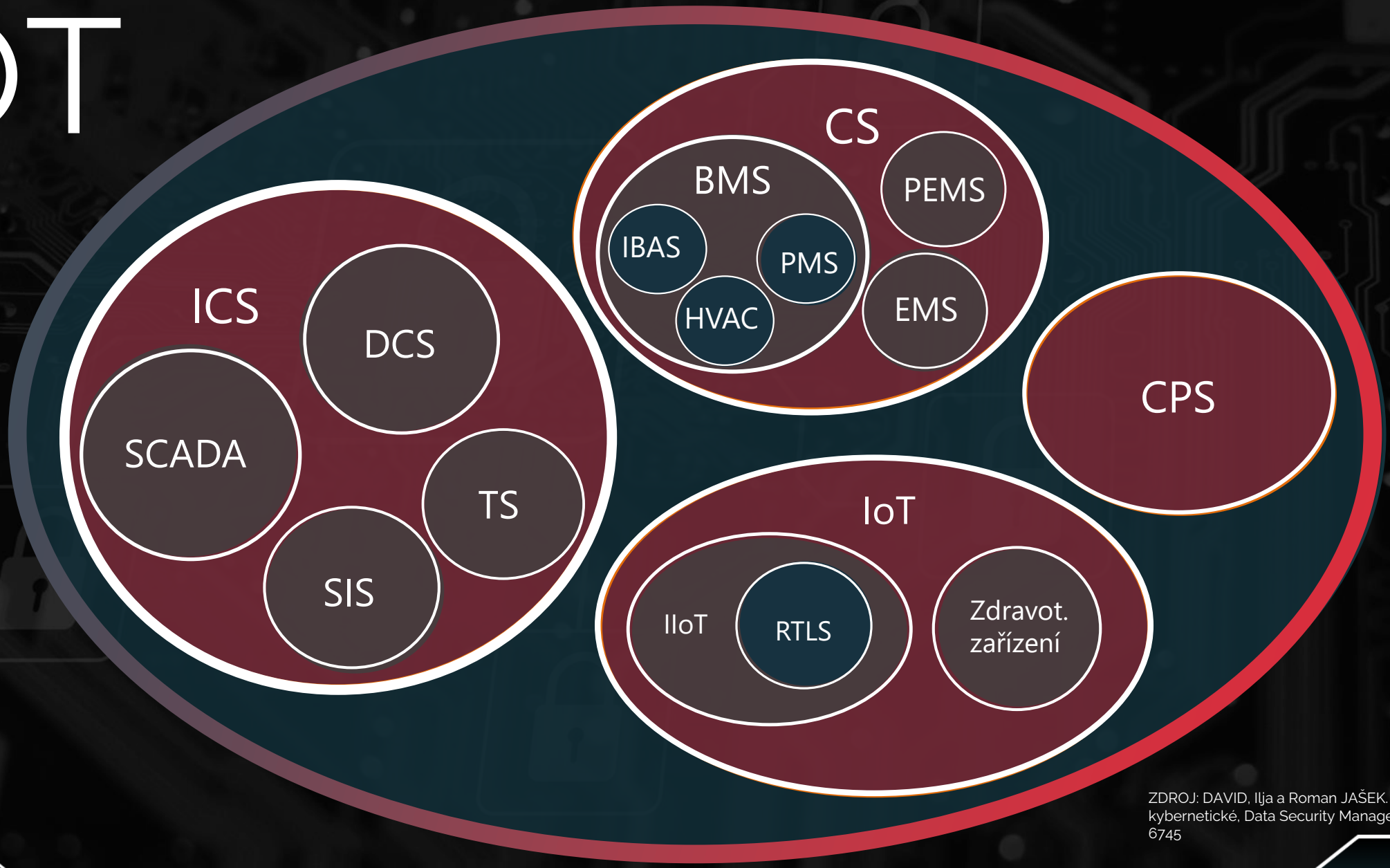
Provozní technologie a jejich rozdíl od technologií informačních

Operational Technologies



ZDROJ: DAVID, Ilja a Roman JAŠEK. Směrem k řešení OT kybernetické, Data Security Management., 10. ISSN 2336-6745

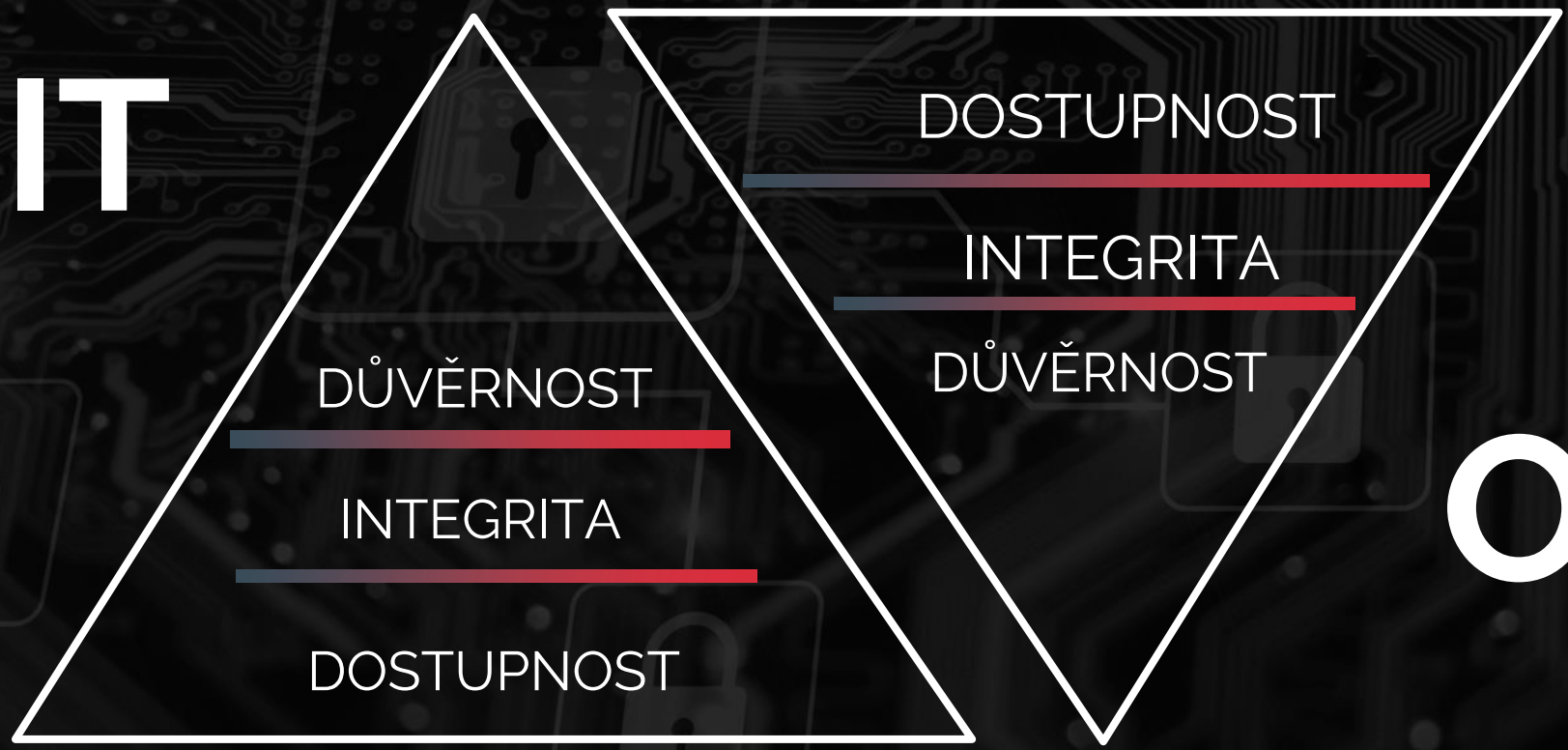
OT



ZDROJ: DAVID, Ilja a Roman JAŠEK. Směrem k řešení OT kybernetické, Data Security Management., 10. ISSN 2336-6745

IT a OT divergence

z pohledu řízení bezpečnosti

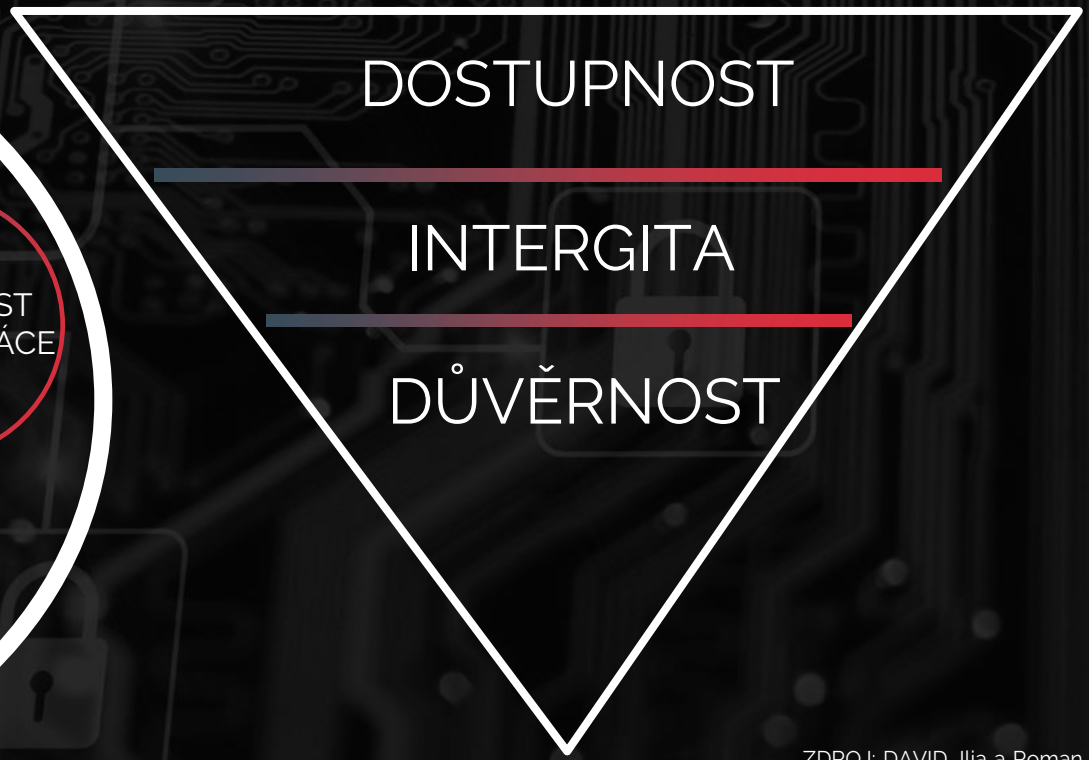


ZDROJ: DAVID, Ilja a Roman JAŠEK. *Konvergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti*. Data Security Management. ISSN 2336-6745

IT a OT divergence

z pohledu řízení bezpečnosti

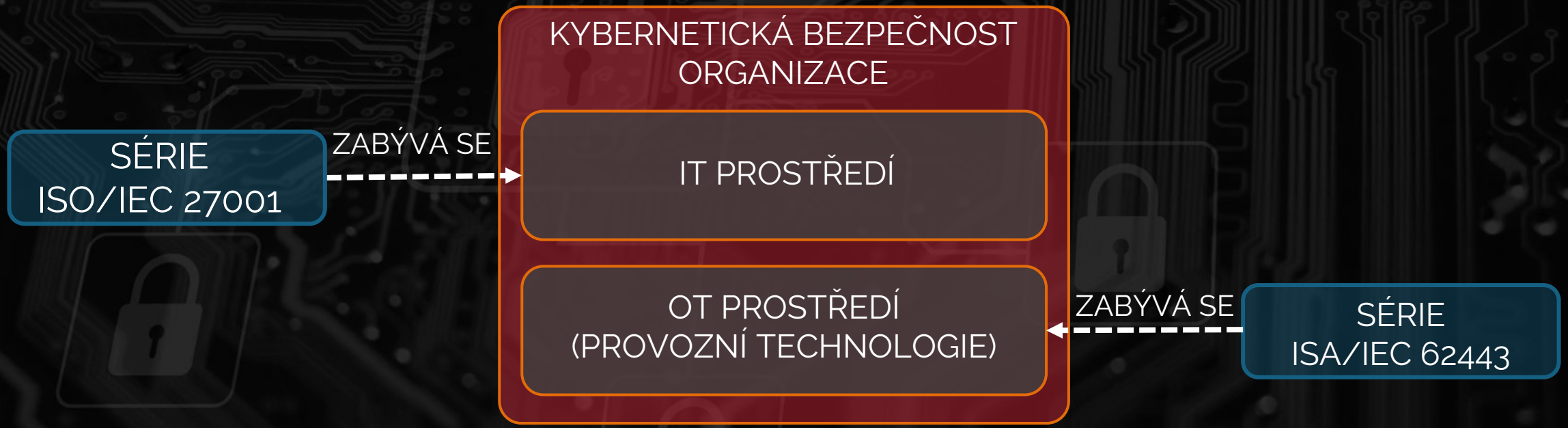
ZDRAVÍ & BEZPEČÍ



ZDROJ: DAVID, Ilja a Roman JAŠEK. *Konvergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti.* Data Security Management. ISSN 2336-6745

IT a OT divergence

z pohledu řízení bezpečnosti



ZDROJ: DAVID, Ilja a Roman JAŠEK. *Konvergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti*. Data Security Management. ISSN 2336-6745

IT a OT divergence

z pohledu řízení bezpečnosti

ZDROJ: DAVID, Ilja a Roman JAŠEK. *Konvergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti*. Data Security Management. ISSN 2336-6745

ISO 27001

Systém řízení informační bezpečnosti (ISMS)

IT Informační bezpečnost

Opatření pro řízení a administrativu procesů

Nedostatek technických řešení

OT není ani zmíněno

Vhodné k řízení kybernetické bezpečnosti OT?

NE

IEC 62443

Systém řízení kybernetické bezpečnosti (CSMS)

OT Kybernetická odolnost

Opatření pro řízení a technická bezpečnostní opatření

PERA model pro OT architektury

Kompenzační opatření

Vhodné k řízení kybernetické bezpečnosti OT?

ANO

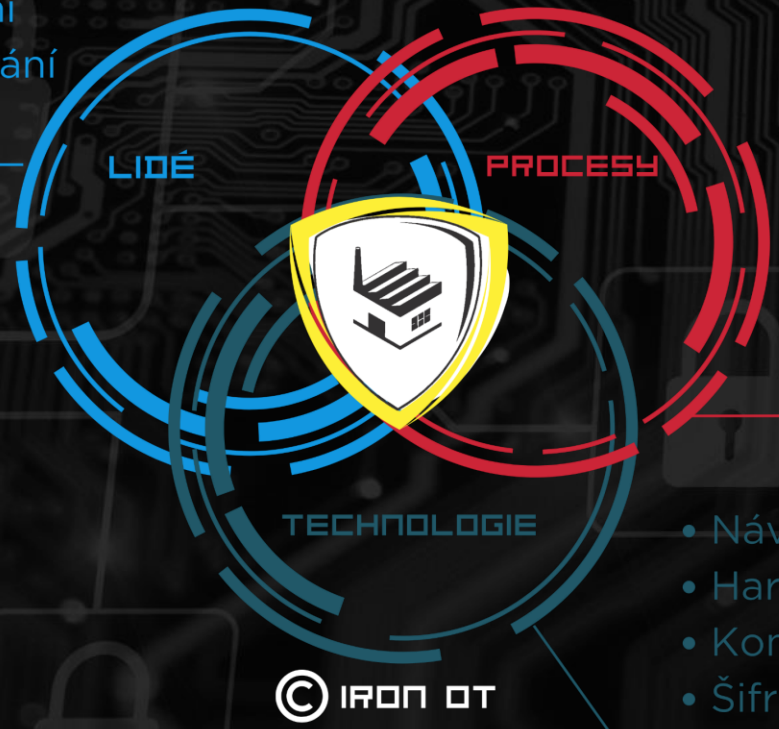
3#

IEC 62443

Praxí ověřená série standardů

Řízení průmyslové kybernetické bezpečnosti

- Školení a informovanost
- Odborné dovednosti a kvalifikace
- Bezpečnostní cvičení
- Autorizace a ověřování
- Fyzická bezpečnost



- Systémy řízení
- Legislativní rámce
- Politiky, standardy, procedury
- Smlouvy s třetími stranami
- Auditní režimy

- Návrh systému
- Hardening systémů
- Konfigurace softwaru
- Šifrovací protokoly
- Detekce a monitorování

> **IEC6 2443** poskytuje **ucelený systém standardů** pro **výrobce**, **provozovatele**, **systémové integrátory** a **poskytovatele služeb** souvisejících s OT

> Cílem je řešit **technologie**, **procesy** a **lidský element** současně

> Kombinace **správných procesů** a **správných technologií** je **klíčová**

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

Řada norem IEC 62443

Obecná kategorie	IEC 62443-1-1	Terminologie, koncepty a modely
	IEC 62443-1-2	Hlavní slovníček pojmů a zkratek
	IEC 62443-1-3	Bezpečnostní a compliance metriky pro systémy
	IEC 62443-1-4	Životní cyklus zabezpečení IACS a případy použití
Bezpečnostní politiky a procedury	IEC 62443-2-1	Založení bezpečnostního programu pro industriální automatizační a kontrolní systémy
	IEC 62443-2-2	Pokyny pro implementaci systému řízení bezpečnosti v rámci IACS systému
	IEC 62443-2-3	Řízení bezpečnostních oprav v prostředí IACS
	IEC 62443-2-4	Požadavky na program bezpečnosti pro poskytovatele služeb IACS
	IEC 62443-2-5	Implementační guidance pro vlastníky IACS aktiv
Bezpečnostní požadavky na systémy	IEC 62443-3-1	Bezpečnostní technologie pro průmyslové automatizační a řídicí systémy
	IEC 62443-3-2	Posouzení bezpečnostních rizik pro návrh systému
	IEC 62443-3-3	Požadavky na bezpečnost systému a bezpečnostní úrovně
Bezpečnostní požadavky na komponenty	IEC 62443-4-1	Požadavky na životní cyklus vývoje bezpečného výrobku
	IEC 62443-4-2	Požadavky technické bezpečnosti pro součásti IACS

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

4# Bezpečná architektura

Bezpečnost je proveditelná

Základní kroky k ochraně OT systémů

1.

Identifikace kritických systémů

- Na co se zaměřit
- Které OT systémy jsou kritické pro továrnu, provoz atd.?

2.

Analýza stávajícího stavu

- Analýza stávajícího a očekávaného stavu (organizace a systémů)
- Typicky IEC62443, ISO27x, nebo např. legislativa (nově NIS2 v EU)

3.

Strategie & Implementace

- Kroky vedoucí k očekávanému stavu
- Síťový a procesní redesign, vzdálená připojení, security zařízení atd.

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

Identifikace kritických systémů

- **Inventarizace systémů**
- Co je **kritické** pro závod, zařízení, továrnu, prvek KI atd.
- Co chránit a s jakým rozsahem **bezpečnostních požadavků**
- **Rozlišit OT od IT systémů** (seskupení pro jednoduchost)
- Konektivita, přístupnost, CIA elementy
- **Scénáře nejhorších případů** (kritičnost)
- Výsledkem je **seznam systémů** s hodnocením kritičnost
- Poté definice **bezpečnostních zón** a zaměřit se dále na to, co je pro organizaci nejkritičtější

System	Location	Vendor	Connected with other systems?	Remote connection?	Possibility to update/upgrade ?	Physical accessibility?
System A	Location 1	Vendor X	Y	Y	Y	Y
System B	Location 2	Vendor Y	N	Y	N	N

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

Bezpečnostní úrovně

- Úroveň bezpečnosti nastavuje rozsah aplikovaných bezpečnostních požadavků na OT systémy (nebo efektivněji na **bezpečnostní zónu**)
- Tímto přístupem lze dosáhnout bezpečnosti pro různé **systémy od více dodavatelů**, starší systémy atd.
- Organizace si může vytvořit **vlastní definici úrovní bezpečnost**i vč. vlastního mat, výpočtu pro každou úroveň
- Doporučují se alespoň **3 úrovně bezpečnosti** (organizace může tento počet zvýšit)
- IEC 62443 pracuje s pěti úrovněmi a **třemi stavy** (SL-T, SL-A, SL-C)

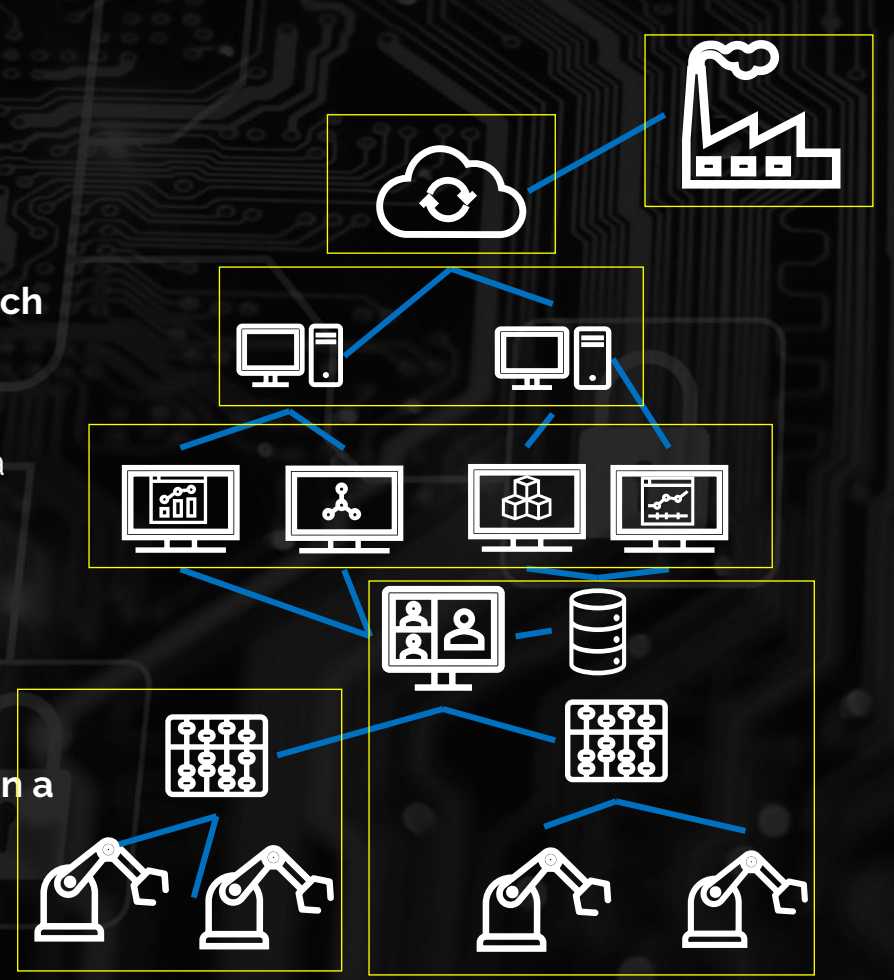
Security Level	Ochrana proti	Skilly	Motivace	Prostředky	Zdroje
SL-0	Nejsou nutné žádné zvláštní požadavky ani bezpečnostní ochrana				
SL-1	Příležitostné popř. náhodné porušení	Žádné útočné dovednosti	Spíše chyby	Neúmyslné	Indivudální
SL-2	Cybercrime, Hackeři	Obecné	Nízké	Jednoduché	Nízké (isolovaný jedinec)
SL-3	Hacktivisté, Teroristé	OT specifické	Střední	Sofistikované (Útok)	Střední (Hackerská skupina)
SL-4	Národní státy	OT specifické	Vysoká	Sofistikované (APT, kampaň)	Veliké (multidisciplinární týmy

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

Bezpečnostní zóny a konduity

- Bezpečnostní **zóny seskupují systémy**, **komponenty**, **zařízení**, **procesy** atd., které sdílejí **stejnou úroveň** bezpečnosti
- Zóny mají definované **úrovně zabezpečení**
- Pro každou úroveň platí jinak **veliká sada bezpečnostních požadavků**
- Cílem je segmentovat různé systémy uvnitř IT/OT sítě a vytvořit **architekturu s prvky a procesy kybernetické bezpečnosti**
- **Modulární**, **škálovatelný** a **flexibilní** systém
- Mělo by být popsáno ve **speciálním nákresu** (nákres **zón a konduitů** – Zones and Conduits drawing)

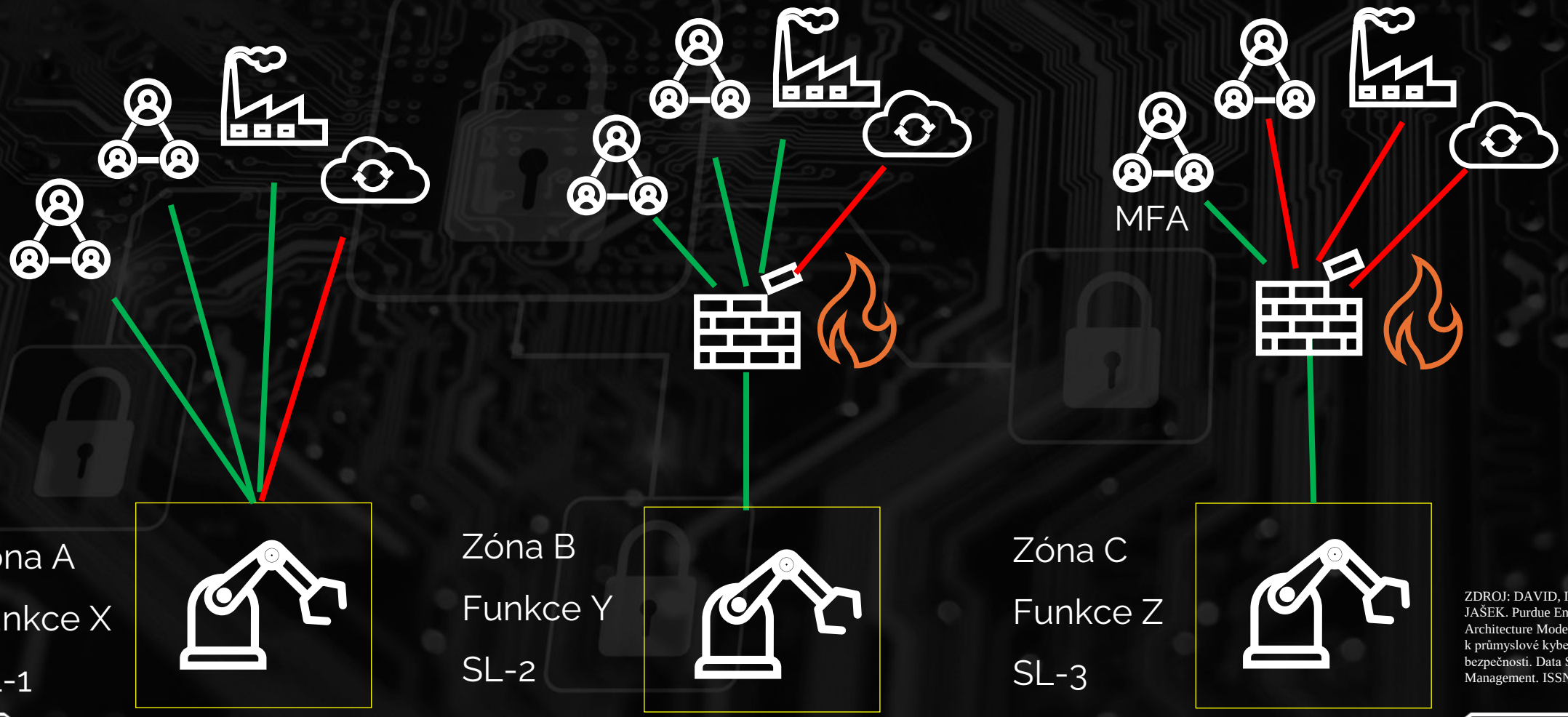
Note: Educational example



ZDROJ: DAVID, Ilja a Roman JAŠEK. Koncept zón a konduitů pro zajištění bezpečnosti provozních technologií (OT) - část 1. Data Security Management. ISSN XXXX

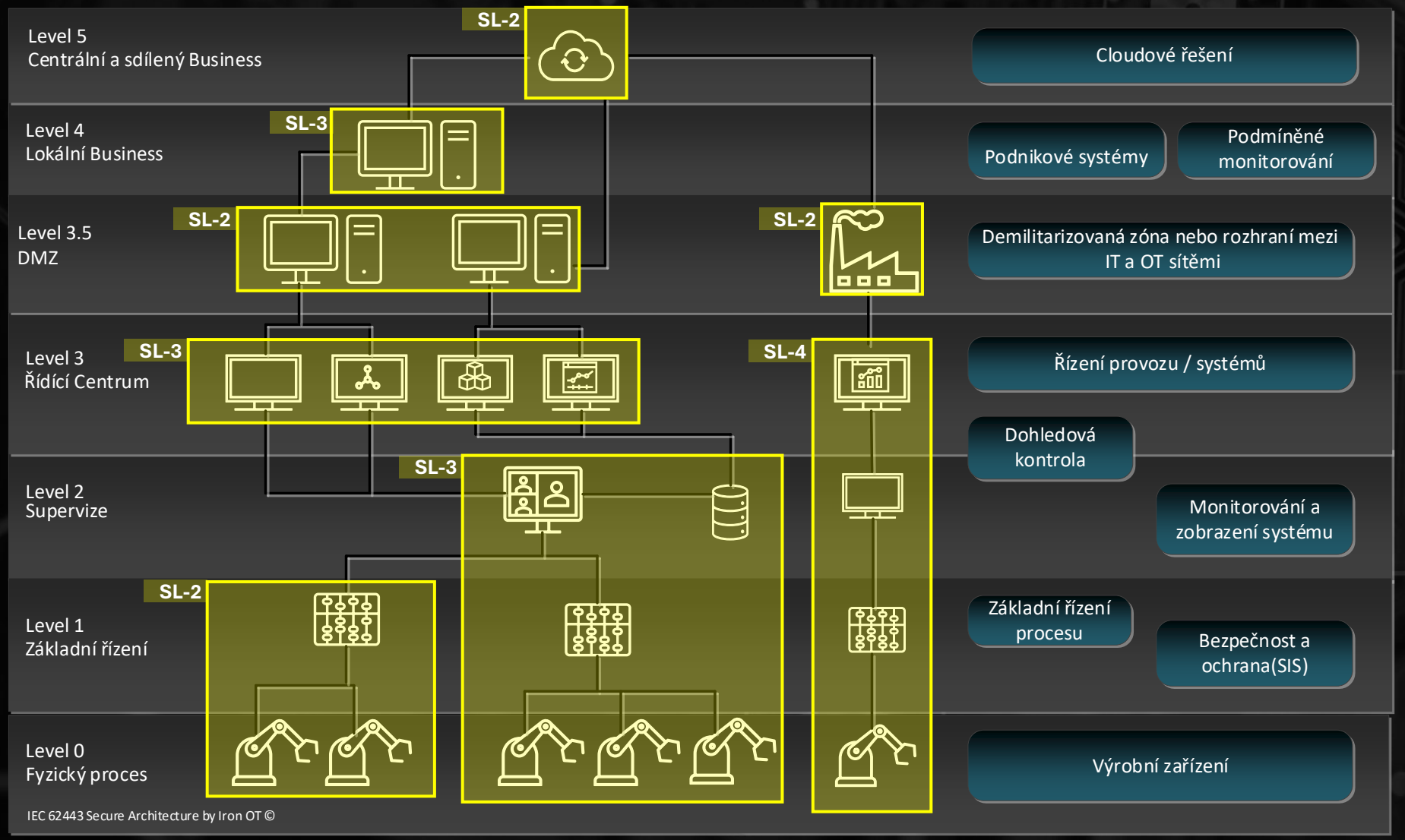
Aplikace bezp. požadavků

Note: Educational example



ZDROJ: DAVID, Ilja a Roman JAŠEK. Purdue Enterprise Architecture Model ve vztahu k průmyslové kybernetické bezpečnosti. Data Security Management. ISSN 2336-6745

IEC 62443 bezpečná architektura



Obvyklá Odpovědnost

OT Guard

IT

Honeywell SCADAfence

Společné IT/OT

wallix

OT/Engineering

Barracuda

IRON OT

COMGUARD

Honeywell

SCADAfence

Monitoring OT sítě

- **Přehled o OT sítích**, komunikačních vzorcích, odhalení potencionálních útoků
- **Asset Management**
- **Monitoring síťového provozu**
- Proaktivně upozorňuje na **zranitelnosti** a **hrozby** v OT síti

- **Centrální management** pro více SCADAfence nebo pro sledování jednotlivých lokalit.
- Agregace informací z několika lokalit a sběr informace z ostatních bezpečnostních systémů
- **Reporting** - zobrazení real-time a generický reportů
- **Podpora standardů** a **legislativa** – IEC62443, NIS2

Reference:

TOYOTA

VESTEL

TARO

Ocenění:

Gartner COOL VENDOR

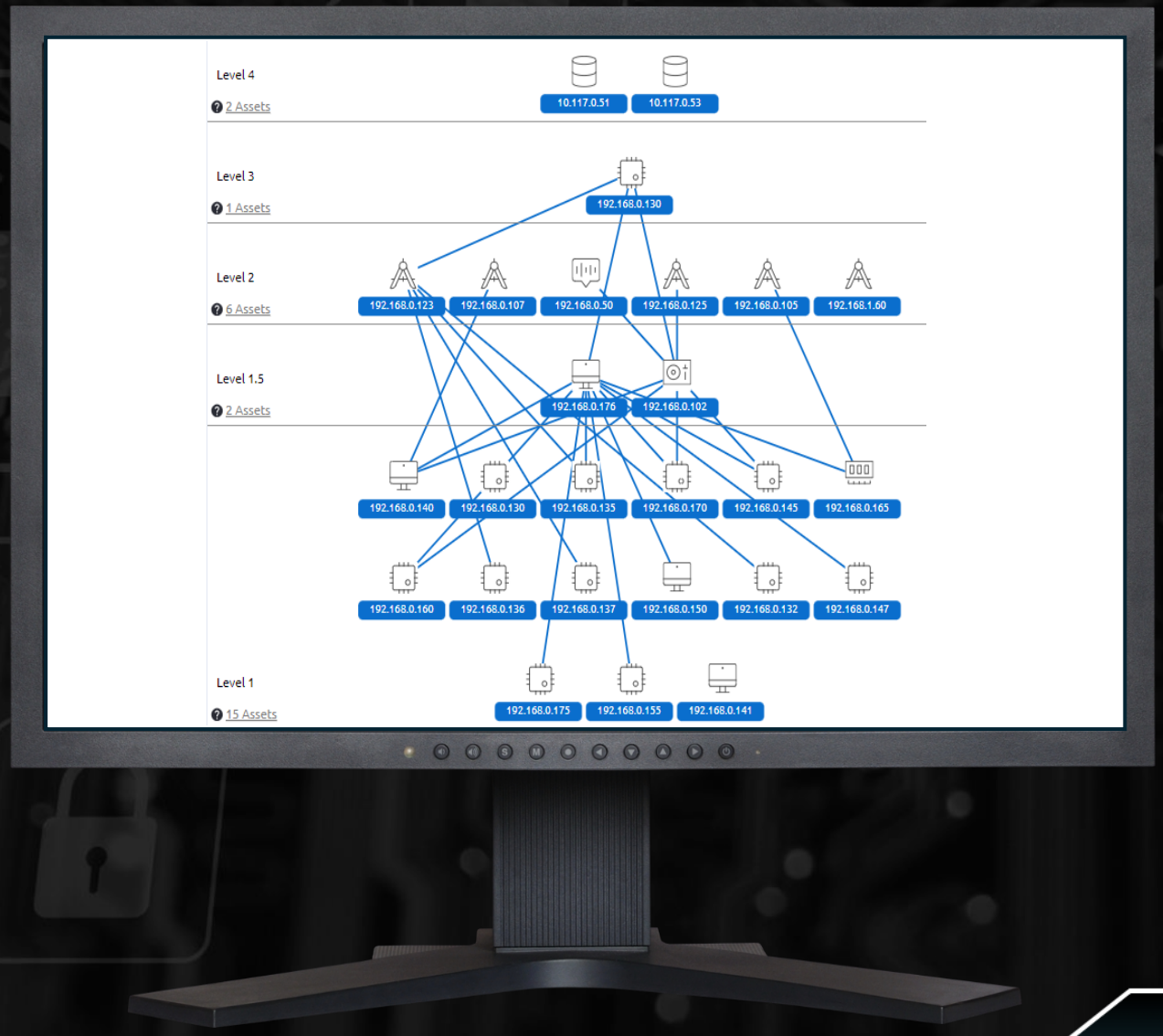
FROST & SULLIVAN

SC awards 2021 WINNER

ISG

Klíčové vlastnosti SCADAfence

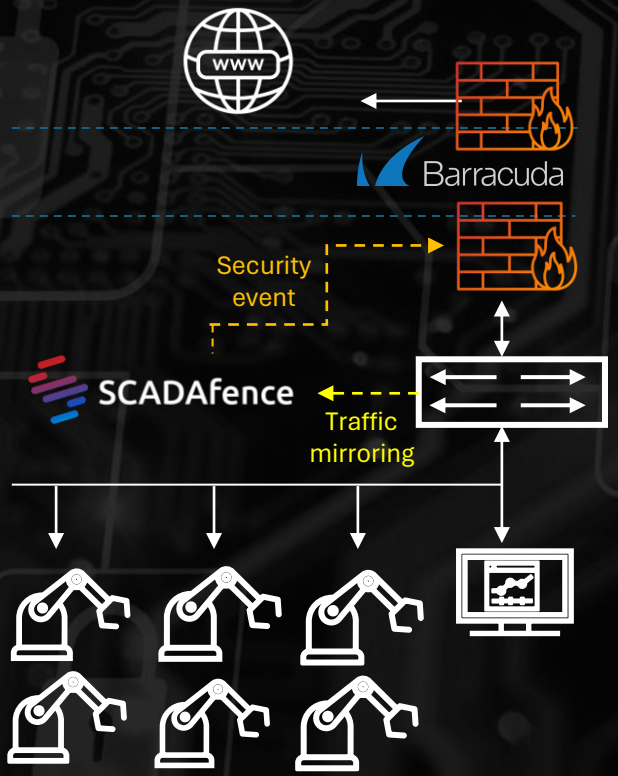
- Detekce hrozeb
- Podpora řízení rizik
- Asset Management
- Bezpečný vzdálený přístup
- Integrace s dalšími nástroji
- Agregace dat z více lokací



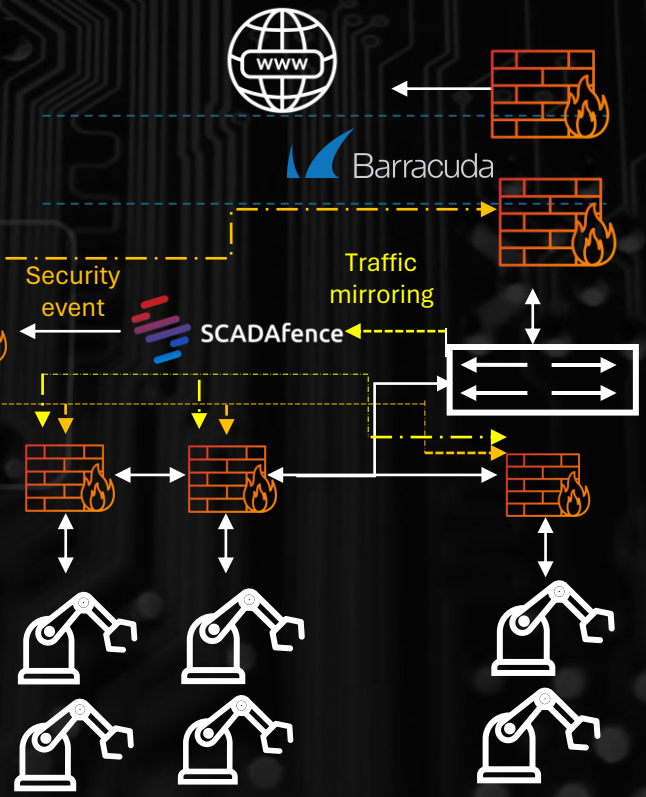
Barracuda Průmyslové firewally

- Hardwarové zařízení do průmyslového prostředí.
- Podpora průmyslových protokolů
- Segmentace průmyslových sítí
- Nativní Honeywell SCADAfence a Barracuda FW integrace
- Integrovatelnost také s jinými zařízení

Detekce hrozeb

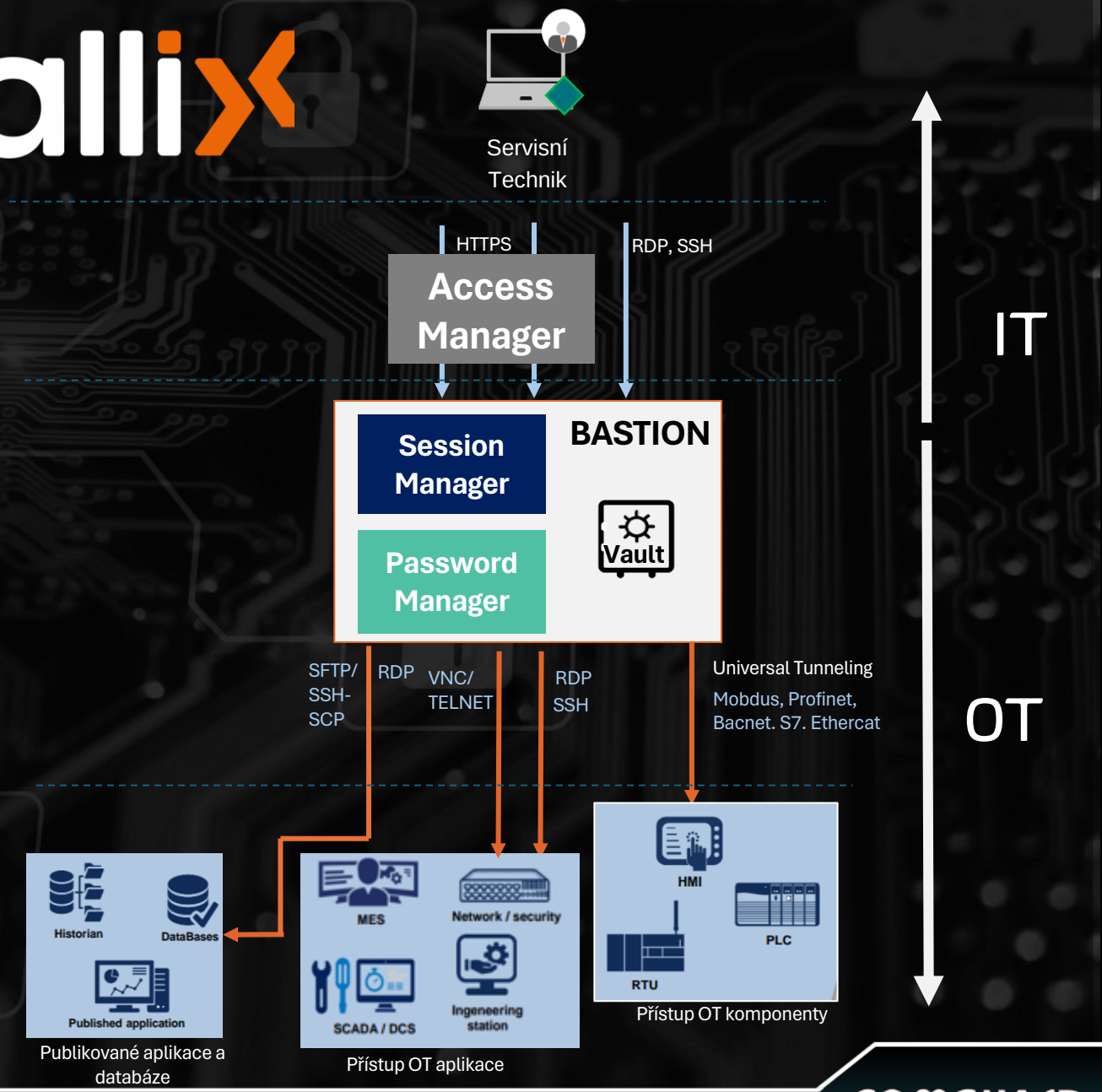


Mikrosegmentace



Řízení přístupů wallix

- Francouzská společnost s mezinárodní působnosti
- Leader v oblasti řízení přístupů PIM / PAM
- Silné zaměření na OT security
- Jednotné řešení pro řízení přístupů do často odlišných OT aplikací



5#
Shrnutí

Shrnutí: implementační strategie OT bezpečnosti

- Na základě předchozích informací lze určit **strategické kroky vpřed** pro zajištění OT bezpečnosti:
  - Krok 1: **posoudit kybernetická rizika** OT systémů, určit které jsou kritické, určit bezpečnostní úrovně a rozdíl mezi stávajícím a očekávaným stavem
  - Krok 2: vytvořit **nákresy zón a konduitů**
  - Krok 3: vytvořit či zlepšit **politiku kybernetické bezpečnosti** IT/OT a související procesy (např. dle IEC 62443);
  - Krok 4: **redesign sítí** a **implementace bezpečnostních zařízení** na ochranu kritických OT systémů (např. OT Guard)
  - Krok 5: zajistit **dlouhodobé řízení**, **monitorování** a **školení** uplatňované bezpečnostní politiky a souvisejících opatření.
- Pokud je to možné, měly by být některé bloky rozděleny podle osvědčených postupů do dvou částí:
  1. **Modelový závod či modelová zóna (nová výrobní linka, retrofit projekt atp.**
  2. **Zbytek závodů či zón**

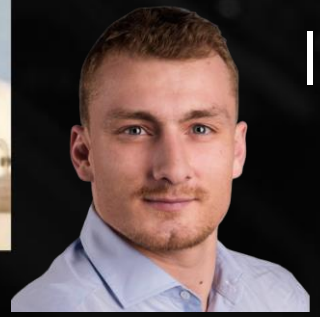
Děkujeme za pozornost!

V oblasti OT Security jsme tu pro Vás

Helena Hrašková

COMGUARD
cyber security masters

helena.hraskova@comguard.cz
+420 770 161 073
Comguard.cz



Ilja David

IRON OT
Secure The Industry Future

Ilja.david@ironot.io
+420 604 421 371
Ironot.io

https://www.linkedin.com/in/ilja-david/

IRON OT

Secure The Industry Future

Top Class Industrial Security, Resilience and Robustness

Iron OT je moderní bezpečnostní společnost nové generace specializující se v rámci Evropské unie na kybernetickou bezpečnost, odolnost a robustnost ochrany provozních technologií (OT) a souvisejících informačních technologií (IT).

- Kritická infrastruktura
- Všechny druhy průmyslů
- Zabezpečení SCADA, DCS, PLC, MES, robotů a další
- IT/OT konvergence

- Systémy řízení kybernetické bezpečnosti
- Posouzení a kompletní návrh řešení bezpečnosti
- Kompletní design bezpečnosti technologických celků
- Implementace frameworků IEC62443 / ISO27001 / NIS2 a mnoho dalších kategorií řešení:

The European Union Security Company

www.ironot.io

COMGUARD

cyber security masters

COMGUARD je Value Added Distributor (B2B) se specializací na IT bezpečnost. Působíme v České republice a na Slovensku. Naše komplexní řešení plně odpovídají potřebám velkých firem, včetně datových center, ale i menších a středních podniků.

- > Bezpečnost koncových stanic
- > Ochrana perimetru
- > Ochrana citlivých dat
- > Vyhodnocování potencionálních rizik
- > Kybernetická bezpečnost v průmyslovém prostředí
- > Správa privilegovaných uživatelů (PAM)
- > Penetrační testování
- > Security Operation Center (SOC)

Pro ochranu operačních technologií nabízí OT Guard, který spojuje několik technologií, které působí synergicky a dokážou pokrýt nejdůležitější oblasti v OT bezpečnosti.

Honeywell SCADAfence

Barracuda

wallix

www.comguard.cz


IRON OT
Secure The Industry Future
COMGUARD
cyber security masters